ABSTRACT

METHOD AND SYSTEM FOR CONDITIONAL ACCESS APPLIED TO PROTECTION OF CONTENT

The invention relates to an access control method controlling access to a broadcast digital dataflow previously scrambled.

The method according to the invention includes the following steps:

On transmission:

- generating an entitlement control message $R\text{-}ECM_c$ for recording the content of the flow as a function of a key KR_c and at least one criterion CRR defining a right to the record,
- generating an entitlement control message $P\text{-}ECM_c$ controlling access to play back the content of the recorded flow as a function of a key KP_c and at least one criterion CRP defining a right to play back, and

on reception:

- analysing the messages $P\text{-}ECM_c$ and $P\text{-}ECM_c$,
- authorising the recording and playback if the criteria CRR and CRP are verified.

Figure 2

APPENDIX 1

Packet IDentifier	Scrambling Control	Payload: Data bytes + padding bytes

An equivalent definition is

```
CAS_PACKET_UNIT()
{
Packet IDentifier                x bits;
Scrambling_Control               2 bits;
Payload z bytes
}
x+2 multiple of 8;
The payload sequence is broken down into Payload()
{
data bytes                       m bytes
padding bytes                    p bytes
}
```

APPENDIX 2

```
CA_descriptor()
{
        descriptor_tag = 0x09          8 bits
        descriptor_length              8 bits
        CA_system_ID                  16 bits
        reserved                       3 bits
        CA_PID                        13 bits
        for (i=0; i<N; i++) {
                private_data_byte      8 bits
```

APPENDIX 3

```
      private data bytes ()
{
   If ECM channel present in the multiplex (see):
{
   ECM_CHANNEL_TAG                          1 byte
channel descriptor indicator SC_ECM
   ECM_XID ;                                1 byte
ECM Stream index in the packet channel
   ECM_CI ;                                 1 byte
version of the crypto-algorithm for the ECM Stream
   ECM_SOID ;                               3 bytes
Reference of the private key set used for the Stream
}
   If SC_ECM channel present in the multiplex:
   (                    // System extension
   SC_ECM_CHANNEL_TAG                       1 byte
channel descriptor indicator SC_ECM
   PPS_ECM_CI;                              1 byte
Version of the crypto-algorithm for the "contents" ECM
   SC_ECM_SOID;                             3 bytes
SOID of SC_ECM
   SC_ECM_PID ;                             x bytes
Identity of the packet channel for SC_ECM
   SC_ECM_XID ;                             1 byte
index of the SC_ECM in the packet channel

      If R_ECM channel present in the multiplex:
      {
      R_ECM_CHANNEL_TAG                     1 byte
channel descriptor indicator R_ECM
      R_ECM_SOID;                           3 bytes
SOID of R_ECM
      R_ECM_PID ;                           x bytes
identity of the packet channel for R_ECM
      R_ECM _ XID;                          1 byte
index of the R_ECM in the packet channel
    }

      If P_ECM channel present in the multiplex:
      {
       P_ECM_CHANNEL_TAG                    1 byte
channel descriptor indicator P_ECM
```

```
        P_ECM_SOID;                                  3 bytes
    SOID of P_ECM
        P_ECM_PID ;                                  x bytes
    identity of the packet channel for R_ECM
        P_ECM_ XID;                                  1 byte
    index of the P_ECM in the packet channel
      }
  }
```